

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans Django

Conditions d'utilisation de ce document : <http://www.certa.ssi.gouv.fr/certa/apropos.html>
Dernière version de ce document : <http://www.certa.ssi.gouv.fr/site/CERTA-2010-AVI-635>

Gestion du document

Référence	CERTA-2010-AVI-635-001
Titre	Vulnérabilités dans Django
Date de la première version	28 décembre 2010
Date de la dernière version	11 janvier 2011
Source(s)	Bulletin de sécurité Django du 22 décembre 2010
Pièce(s) jointe(s)	Aucune

TAB. 1 – Gestion du document

Une gestion de version détaillée se trouve à la fin de ce document.

1 Risque

- Déni de service à distance ;
- atteinte à la confidentialité des données.

2 Systèmes affectés

- Django versions 1.1.x inférieures à 1.1.3 ;
- Django versions 1.2.x inférieures à 1.2.4.

3 Résumé

Deux vulnérabilités, l'une permettant un déni de service et l'autre d'obtenir des informations confidentielles, ont été corrigées dans *Django*.

4 Description

Une mise à jour de *Django* corrige deux vulnérabilités. La première permet à une personne malveillante connaissant bien le modèle utilisé par l'application, d'obtenir des informations confidentielles. La seconde per-

met à un attaquant d'épuiser les ressources du serveur en lui envoyant des requêtes de changement de mots de passe spécialement conçues.

5 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Bulletin de sécurité Django du 22 décembre 2010 :
<http://www.djangoproject.com/weblog/2010/dec/22/security>
- Bulletin de sécurité Ubuntu USN-1040-1 du 07 janvier 2011 :
<http://www.ubuntulinux.org/usn/usn-1040-1>
- Référence CVE CVE-2010-4534 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-4534>
- Référence CVE CVE-2010-4535 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-4535>

Gestion détaillée du document

28 décembre 2010 version initiale.

11 janvier 2011 ajout des références au bulletin Ubuntu et aux CVE.